

Internetin turvallisuus

Comer: 9, 30

vanha kirja ss. 576-646

Sisältö

- Kertaus: turvallisuuden osa-alueet
- Palomuurit
- Yksityisverkot (Virtual Private Network, VPN)
- Internet Protocol Security (IPsec)
 - Luottamuksenhallinta

Turvallisuus

- Luottamuksellisuus (confidentiality)
- Eheys (integrity)
- Saatavuus (availability)
- Pääsynvalvonta (access control)
- Todennus ja valtuutus (authentication and authorization)
- Kiistämättömyys (non-repudiation)

Kryptologia (cryptology)

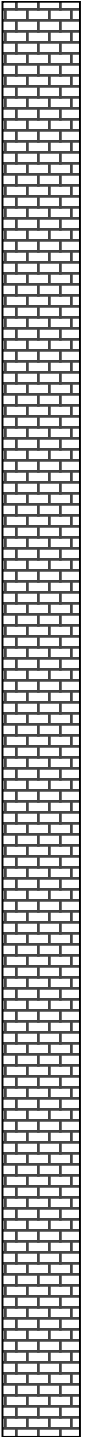
- Symmetrinen ja julkisen avaimen salakirjoitus
- Digitaaliset allekirjoitukset
- Kryptograafiset tiivistefunktiot (hash function)
- Message Authentication Code (MAC)
- Satunnaislukugeneraattorit

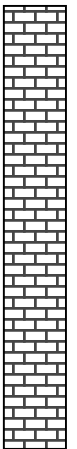
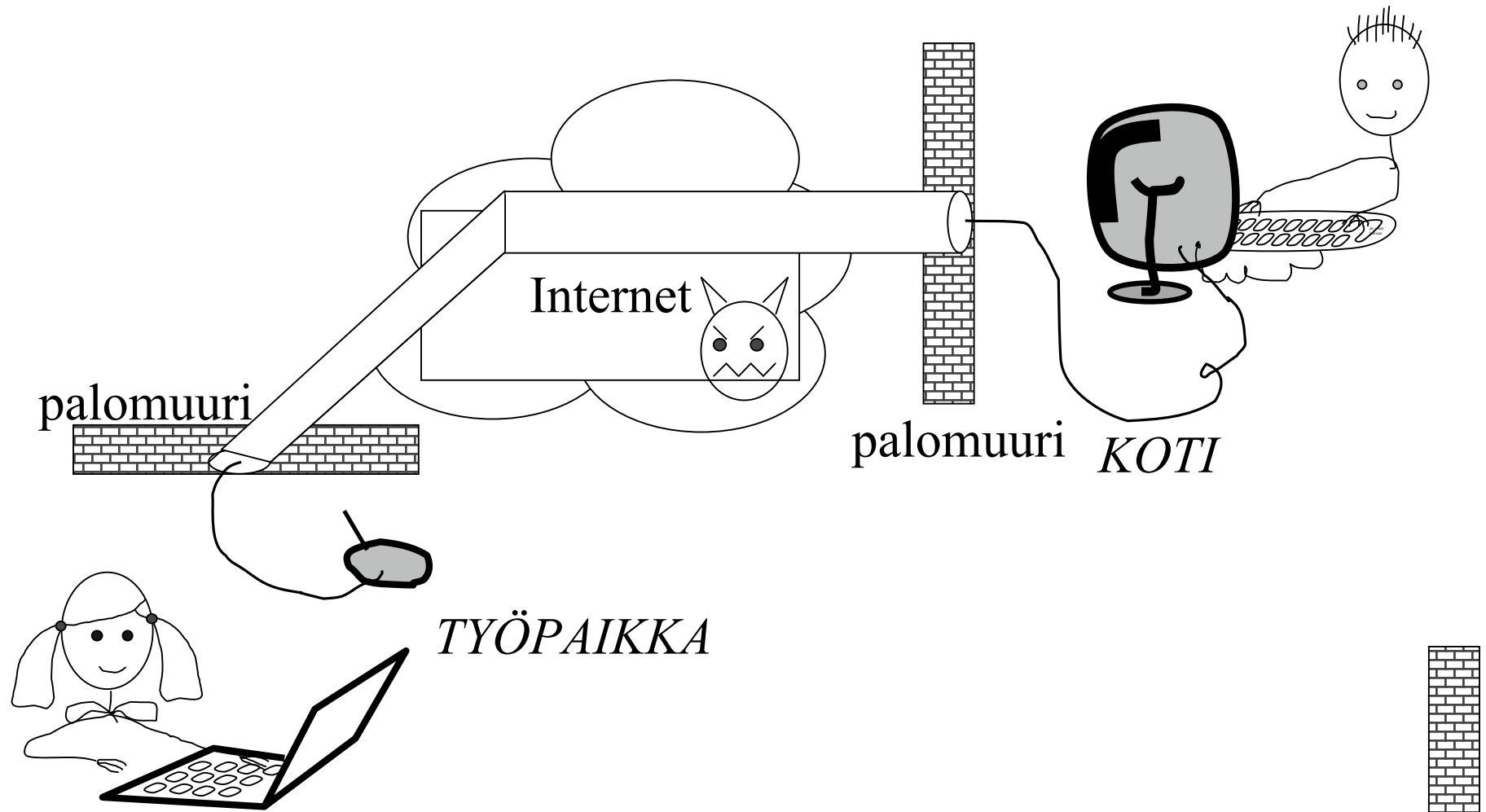
Palomuurit

Sanna Suoranta
T-110.4100@tkk.fi

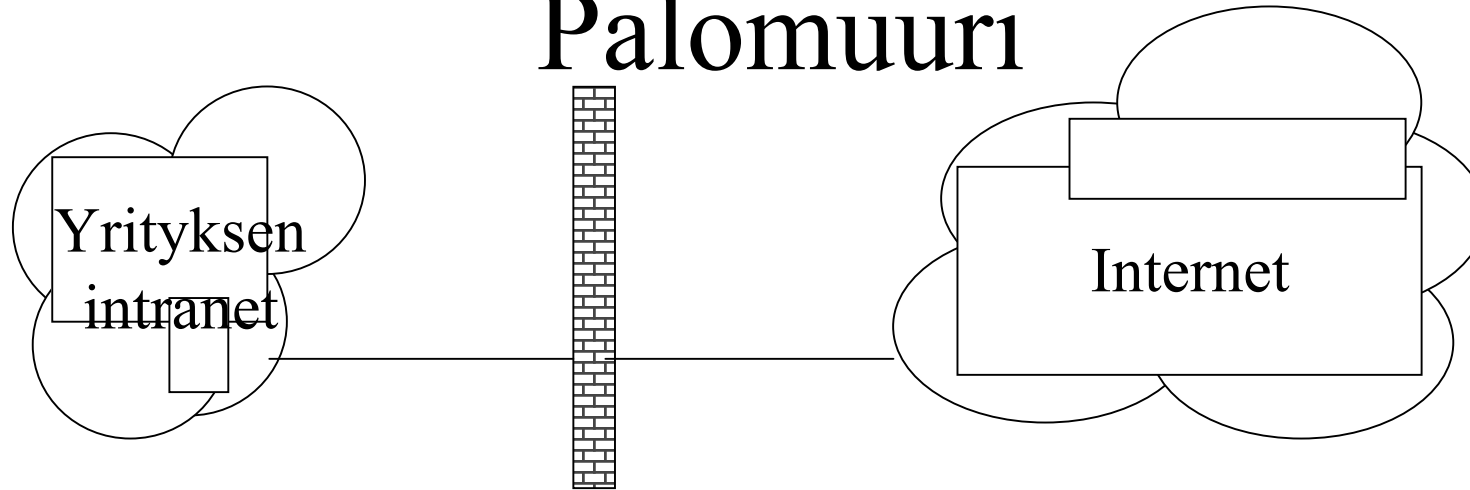
T-110.4100 Tietokoneverkot
<https://noppa.tkk.fi/noppa/kurssi/t-110.4100>

5
24.9.2009

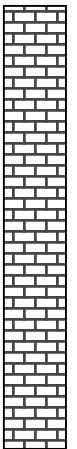




Palomuuuri

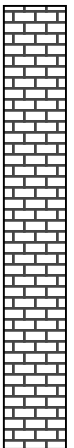


- Erottaa “sisäverkon” ja “ulkoverkon”
 - Toteuttaa pääsypolitiikan
 - Piilottaa sisäverkon rakenteen (esim. yhteistoiminta NAT:n kanssa)
 - Seuranta ja hälytykset



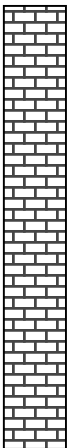
Verkkokerroksen palomuurit

- Kutsutaan myös pakettipalomuureiksi (packet filter)
- Pääsypäätös perustuu IP-osoitteisiin ja TCP/UDP-portteihin
- Estää kaikki tietosähkeet, paitsi tietyt osoitteet, portit ja protokollat
 - Jokainen paketti käsitellään erikseen
- Yksinkertainen ja tehokas
- Voidaan toteuttaa reitittimessä
 - Ei standardeja, toteutukset valmistajakohtaisia



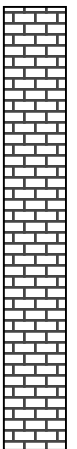
Verkkokerroksen palomuurien ongelmat

- Palomuuuri ei ymmärrä yhteyden sisältöä
- Tarvitaan yksityiskohtaiset tiedot verkon palveluista
- Uusien palveluiden mukanaanotto määriteltävä aina erikseen
- Yksityiset portit (asiakas-palvelin-yhteydet)
- Valtuuttamattoman liikenteen tunnelointi mahdollista



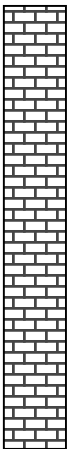
Sovelluskerroksen palomuurit

- Välittäjäpohjaiset palomuurit (proxy-based)
- Ymmärtävät käytettäviä sovelluksia
- Monimutkaisempia mutta muutoskykyisempiä



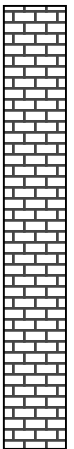
Valvonta

- Eng. surveillance tai monitoring
- Tarkoitus on huomata ongelmat ja murtoyritykset
- Aktiivinen: esim. Lähetetään sähköpostia ylläpitäjälle
- Passiivinen: kirjoitetaan lokiin
- Huom. Jos joku on päässyt murtautumaan järjestelmään, hän saattaa pystyä myös muuttamaan lokia

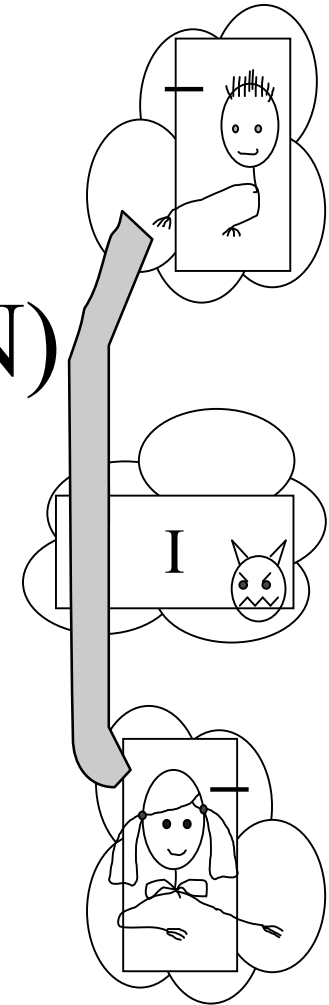


Yhteenveto palomuuureista

- Palomuurit estävät valtuutonta pääsyä verkkoon ja sen laitteisiin
 - Palomuurin hallinta vaatii tietämystä
 - Henkilökohtaiset palomuurit?
- Palomuurit eivät ratkaise kaikkia tietoturvan palveluita

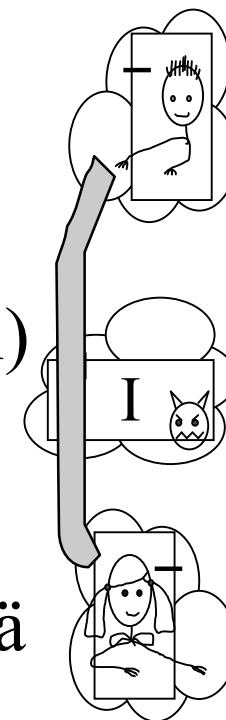


Yksityisverkot (Virtual Private Network VPN)



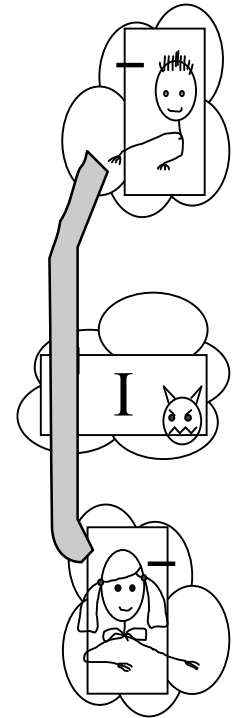
Yksityisverkot (VPN)

- Yhteys organisaation sisäverkkoon Internetin yli
 - Ei varata yksityistä kanavaa (vuokrattu linkki) yhdistämään verkkoja
- Toteutetaan tunneloimalla ja salaamalla
 - suojataan luottamuksellisuutta ja yksityisyyttä
- Useita valmistajakohtaisia toteutuksia
 - sekä rauta- että ohjelmistototeutuksia



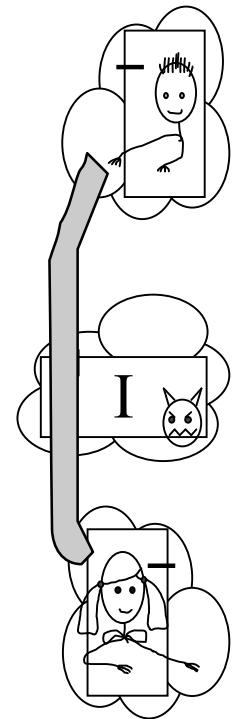
Ominaisuudet

- Turvapolitiikka
 - millaiset yhteydet sallitaan
- Pääsynvalvonta
 - kuka voi ottaa yhteyttä
- Turvalliset yhteydet
 - mitä turvapalveluita käytetään
- Tarvitaan jonkinlainen valtuutusmenetelmä



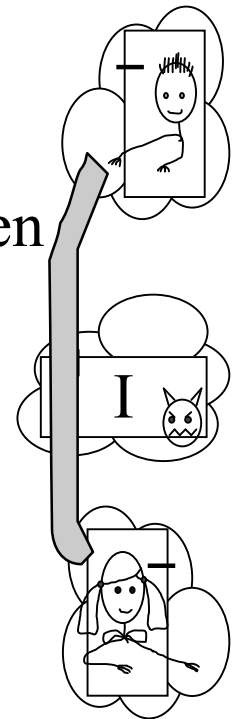
Käyttäjän tunnistus

- Perinteiset salasanat (heikko)
- Kertakäyttösalasanat (one-time password OTP)
 - S/Key määritelty: RFC 2289
 - Salaisuus (secret passphrase) OTP:n generointiin
- Autentikoinnin asiakas-palvelin menetelmät
 - Password Authentication Protocol (PAP)
 - Point-to-Point (PPP) protokollan tapa
 - Salasanoihin pohjautuva kaksisuuntainen kädenpuristus
 - Ei turvallinen, käytetään selväkieltä



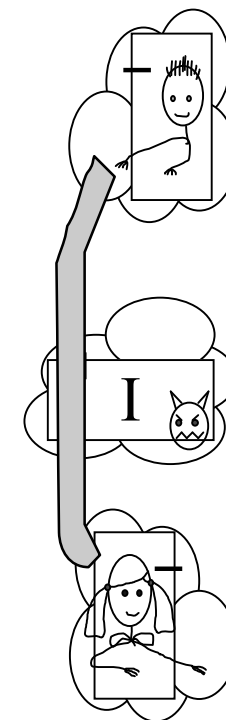
Käyttäjän tunnistus

- Challenge Handshake Authentication Protocol (CHAP)
 - Kolmitiekättely: haaste-vaste-hyväksyntä
 - Perustuu jaettuun salaisuuteen asiakkaan ja palvelimen välillä
- Terminal Access Controller Access-Control System (TACACS)
- Remote Authentication Dial-in User Service (RADIUS)
 - Keskitetty palvelin
- Diameter (kehitetty RADIUSista)
- Rautapohjaiset järjestelmät esim. tokenit



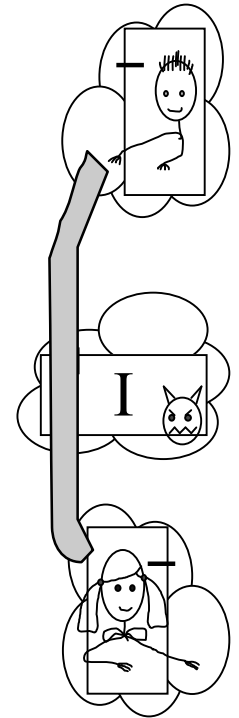
VPN-tunneli läpi Internetin

- IPsec ja turva-gateway
- Point-to-Point Tunneling Protocol (PPTP)
 - PPTP käyttää (MS-)CHAP autentikointia (Windows)
- Layer Two Tunneling Protocol (L2TP)
 - RFC 2661
 - Perustuu PPTP:n ja Ciscon L2F, sekä IPseciin

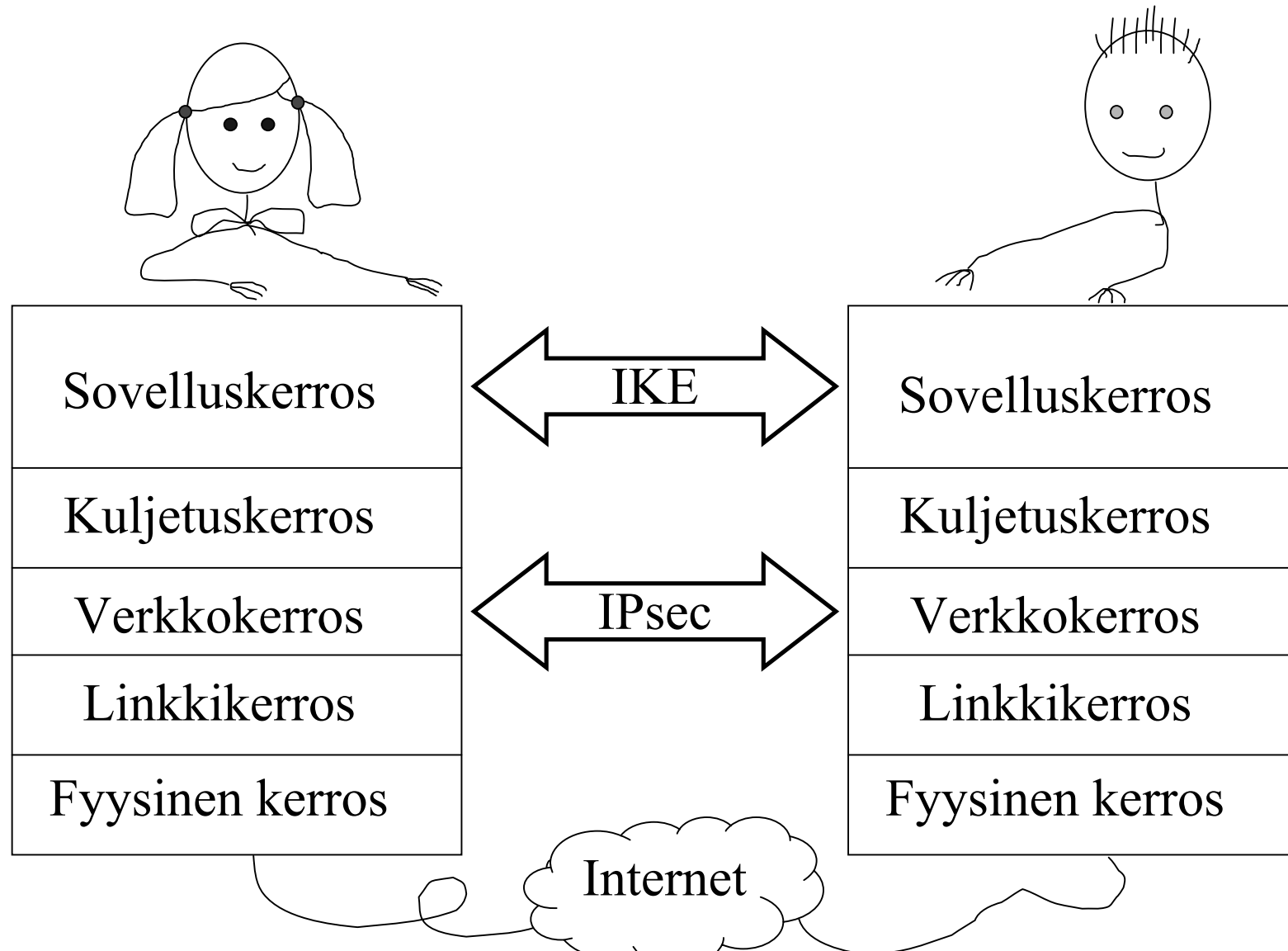


VPN-yhteenveto

- Yksityisverkot (Virtual Private Network) on konsepti
- Useita erilaisia toimittajakohertaisia ratkaisuja saatavilla
- Voidaan suunnitella soveltumaan hyvin tietyn organisaation tarpeisiin



Internet Protocol Security (IPsec)



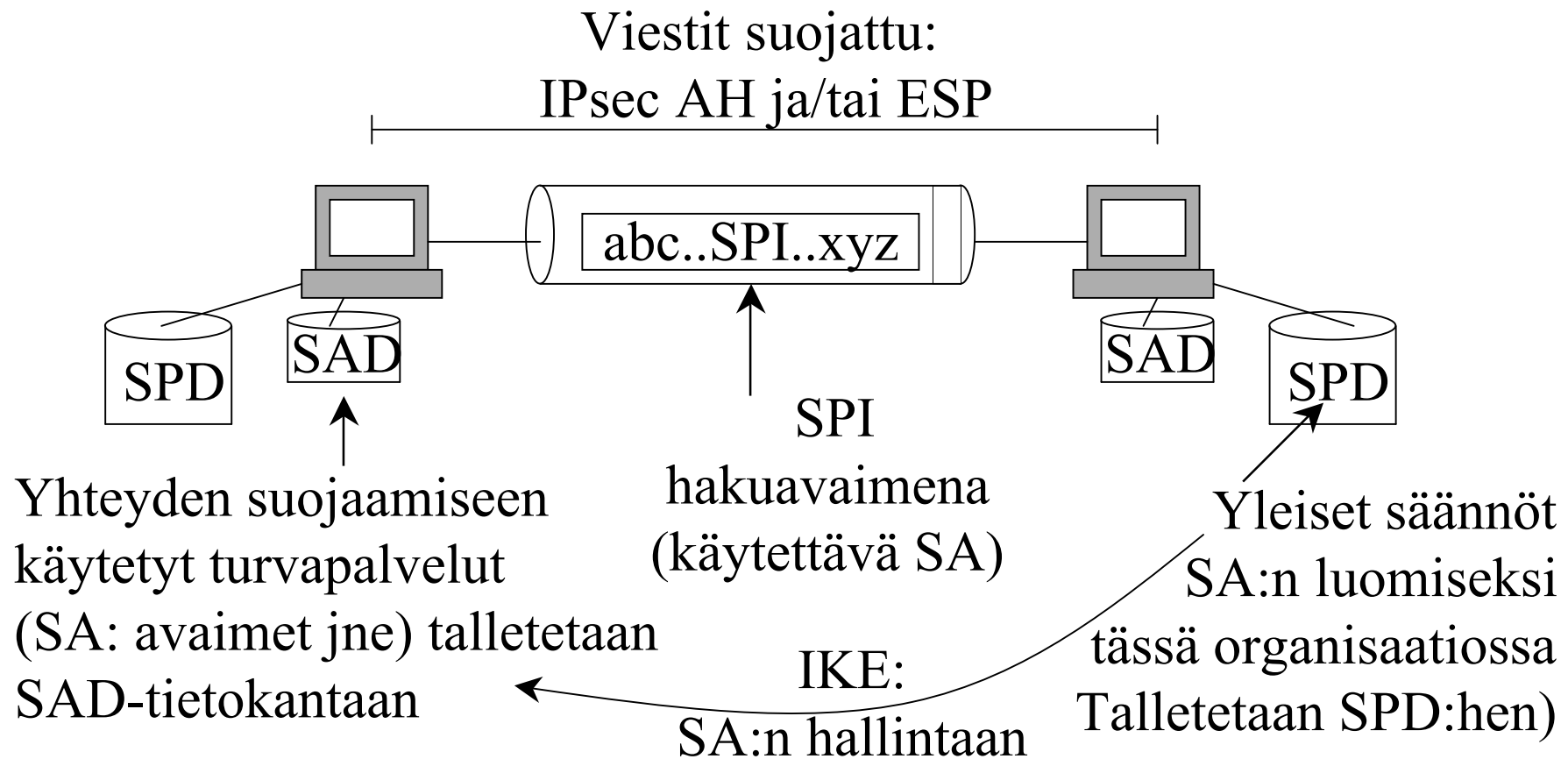
IP Security (IPsec)

- Tiedon suojaus ja suojaustavan neuvottelu
 - Authentication Header (AH)
 - Encapsulating Security Payload (ESP)
 - Internet Key exchange (IKE)
- Kuljetus (transport) ja tunnelointi (tunneling)
 - Kahden isäntäkoneen, kahden turva-gatewayn tai turva-gatewayn ja isäntäkoneen välillä
- Toimii sekä IPv4:n että IPv6:n kanssa
 - Silti aivan sama protokolla

IPsec tarjoaa

- Pääsynvalvonta (access control)
- Yhteydetön eheys (connectionless integrity)
- Tiedon alkuperän todennus (data origin authentication)
- Suojaus toistoa vastaan
- Luottamuksellisuus (confidentiality)
- Rajoitettu vuon luottamuksellisuus
 - Mitä nämä oikeasti tarkoittavat IPsecin kohalla?

IPsec-kehys (framework)



IPsec Framework (2)

- SA: Turva-assosiaatio (security association)
- SPD: Turvapolitiikkatietokanta (security policy database)
- SAD: Turva-assosaatietietokanta (security association database)
- IKE: Avaintenhallinta (key management)
- AH: Todennusotsikko (authentication header)
- ESP: Salausotsikko (encapsulating security payload)

Turva-assosiaatio (SA)

- SA määrittelee käytetyt turvapalvelut
 - Käytetty turvaprotokolla, algoritmit ja mekanismit
 - Joita käytetään kahden päätepisteen välisellä yhteydellä yhteen suuntaan
- SA:n tunniste:
 - Security Parameter Index (SPI), kohteen IP-osoite ja turvaprotokollan tunniste

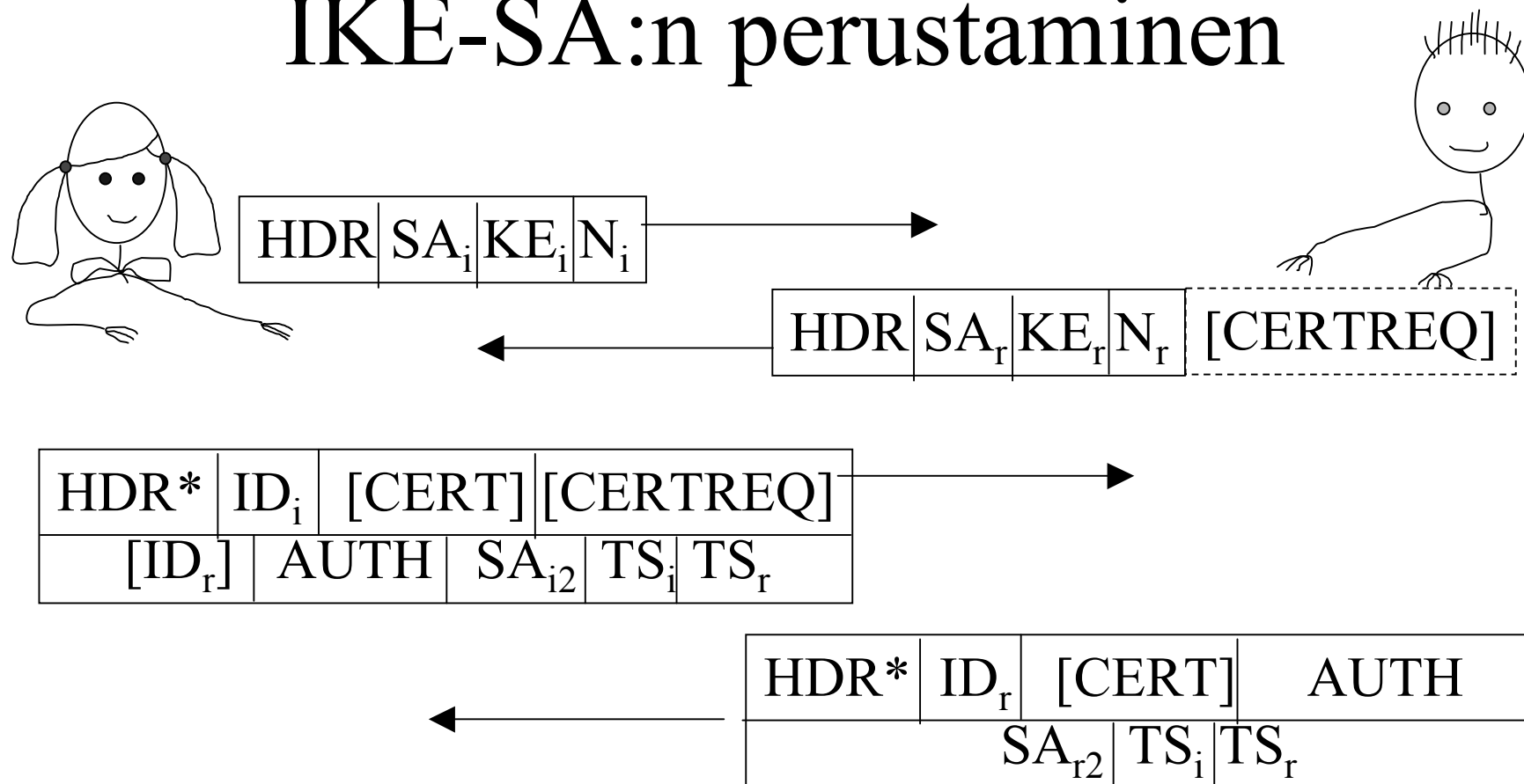
SA- ja turvapolitiikkatietokannat

- Security Association Database (SAD)
 - Kaikkien käytössä olevien yhteyksien SAt
- Security Policy Database (SPD)
 - (Organisaatiossa) käytössä olevat turvapalvelut: millaiset SAt ovat sallittuja
 - Kaikkien yhteyksien turvallisuuden hallinta
- IPsec ei määrittele kuinka tietokantoja käytetään
 - Paikallinen päätös (toimittajakohtaista)

Internet Key Exchange (IKE)

- IPsecin avaintenvaihto- ja SA:n hallintaprotokolla
- Käyttää Diffie-Hellman avaintenvaihtoa
- Ensimmäisessä vaiheessa: SAt päätepisteiden välille
 - osapuolten tunnistus ja neuvottelun turvaaminen
- Toinen vaihe: SA IPsec-yhteydelle
- Ei tarvita kolmatta osapuolta tai palvelinta
- Nykyinen versio IKEv2

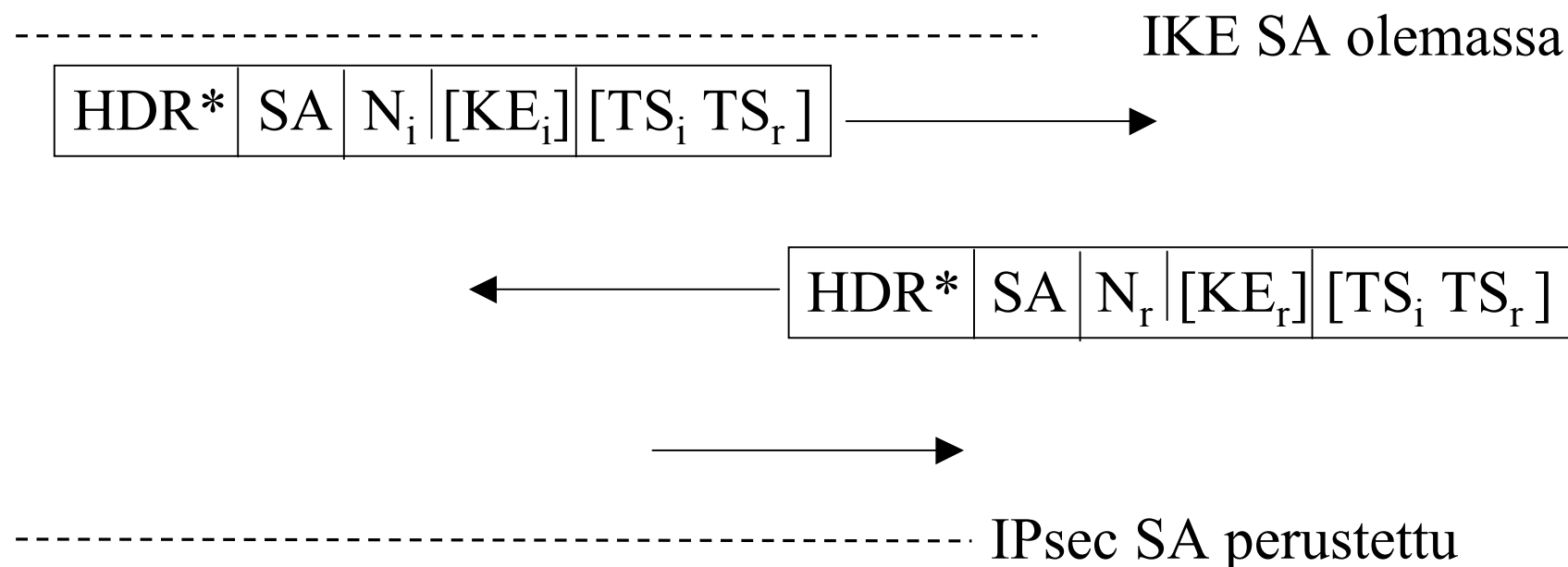
IKE-SA:n perustaminen



** kaikki otsikon jälkeen on suojattu*

IKE-SA perustettu

IPsec-SA:n perustaminen



IKEv2 - Otsikko

0	8	16	24	31
INITIATOR'S SPI (64 bits)				
RESPONDER'S SPI (64 bits)				
NEXT PAYLOAD	MjV	MnV	EXCHANGE TYPE	FLAGS
MESSAGE ID				
LENGTH				

- SPI: lähettäjä valitsee (vastaanottajan SPI aluksi 0)
- Seuraava kuorma (next payload)
- Viestinvaihtotyyppi määrittelee viestit
 - 0-33 varattu, 34 SA init, 35 auth, 36 child SA, 37 Informational, 38-239 IANA, 240-255 private

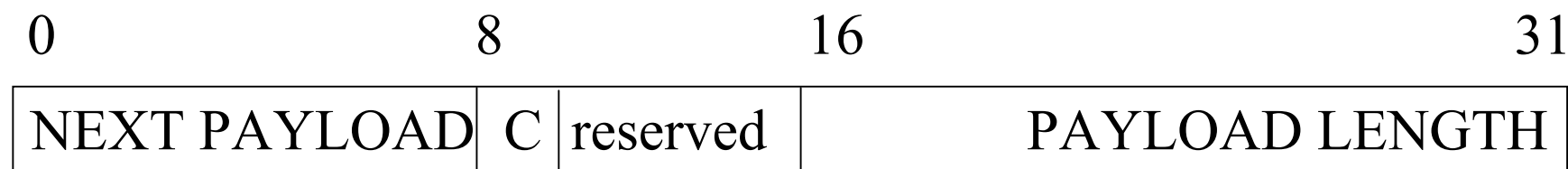
IKEv2 - Otsikko

- Kaksi versionumeroa, major ja minor
 - ylin ja alin ”ymmärrettävä” versio
- Liput
 - (3.) I(nitiator)=1, alkuperäinen 1. lähettäjä lähettää
 - (4.) V(ersion)=1, jos ymmärretään uudenpaakin
 - (5.) R(esponse)=1, jos viesti on vastaus
 - (0.-2. ja 6.-7.) = 0 (varattu)

IKEv2 - Otsikko

- Message ID
 - Käytetään vaiheessa 2 (eli IPsecin SA:ta luotaessa)
 - Lähettäjän valitsema satunnaisluku
 - Käytetään identifioimaan SA neuvottelun aikana
- Pituus
 - Otsikko+hyötykuormat oktetteina
 - Huom: salaus saattaa pidentää pakettia

IKEv2- Yhteinen alku viesteille ja optiot



- Kaikki ISAKMP-hyötykuormat alkavat

TLV:

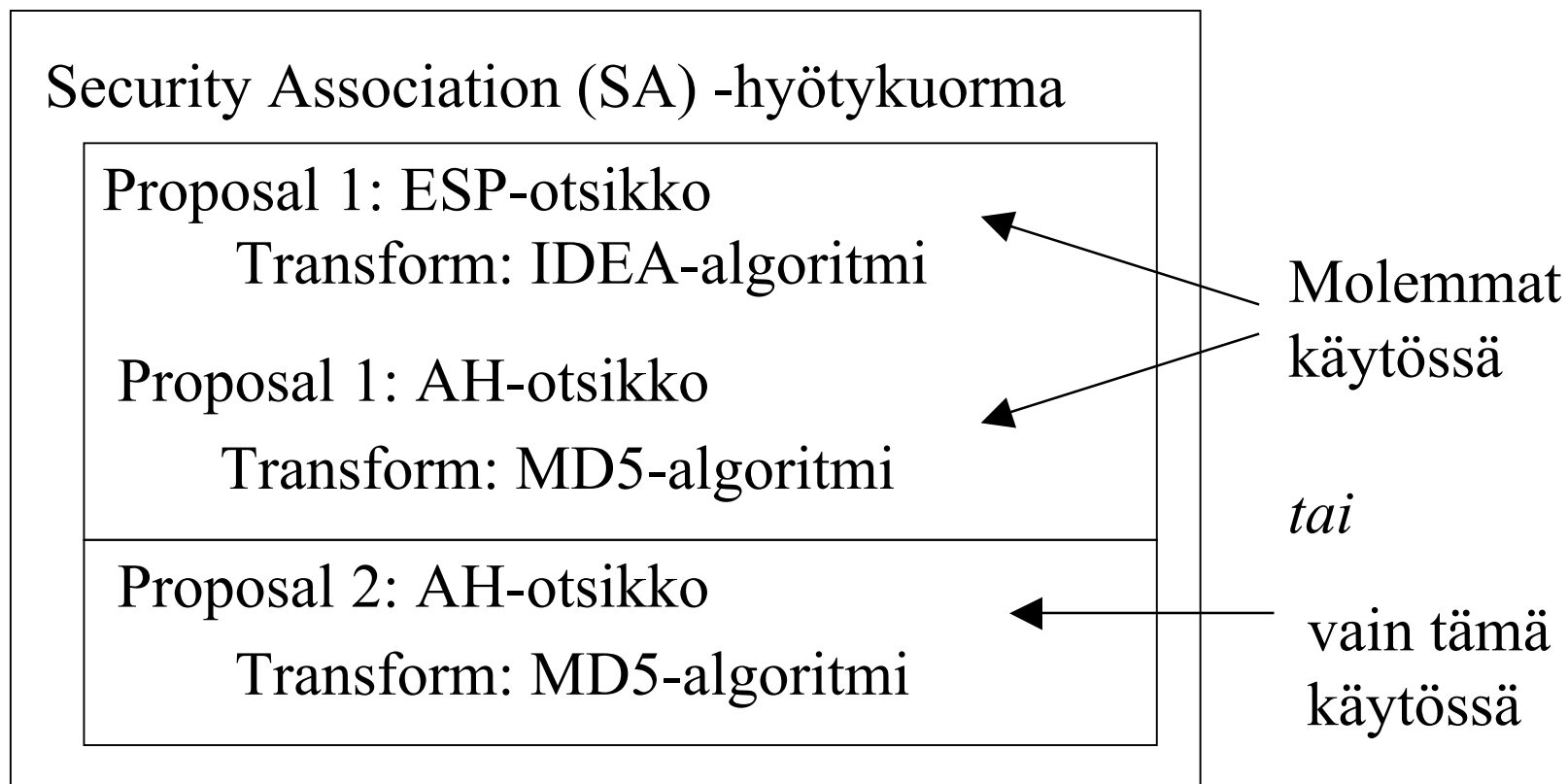


TV:



- Atribuutteja käytetään SA-määrittelyssä
 - joko TLV- tai TV-tyyppiä
 - Ensimmäinen bitti merkitsee

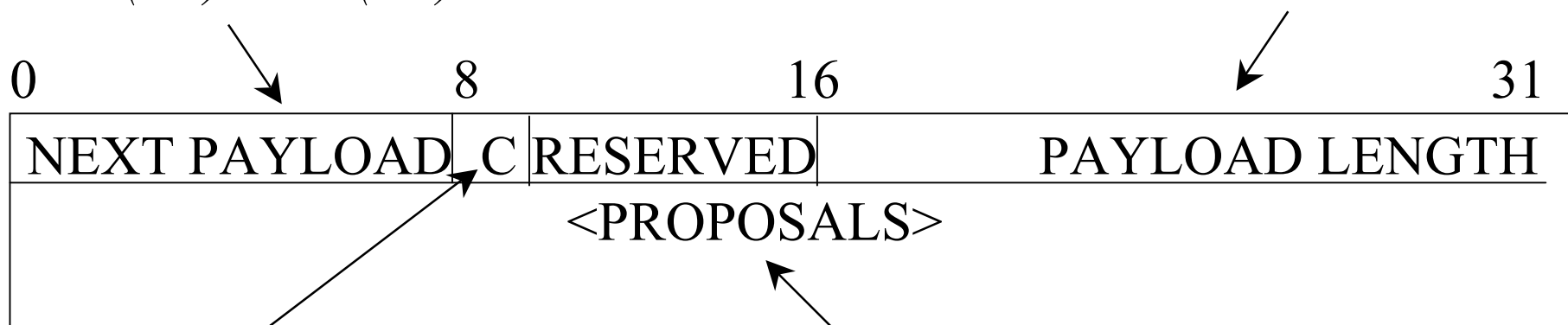
Turva-assosiaatio (SA)



Security Association Payload (SA)

*Seuraava otsikko
ei P (=2) tai T (=3)*

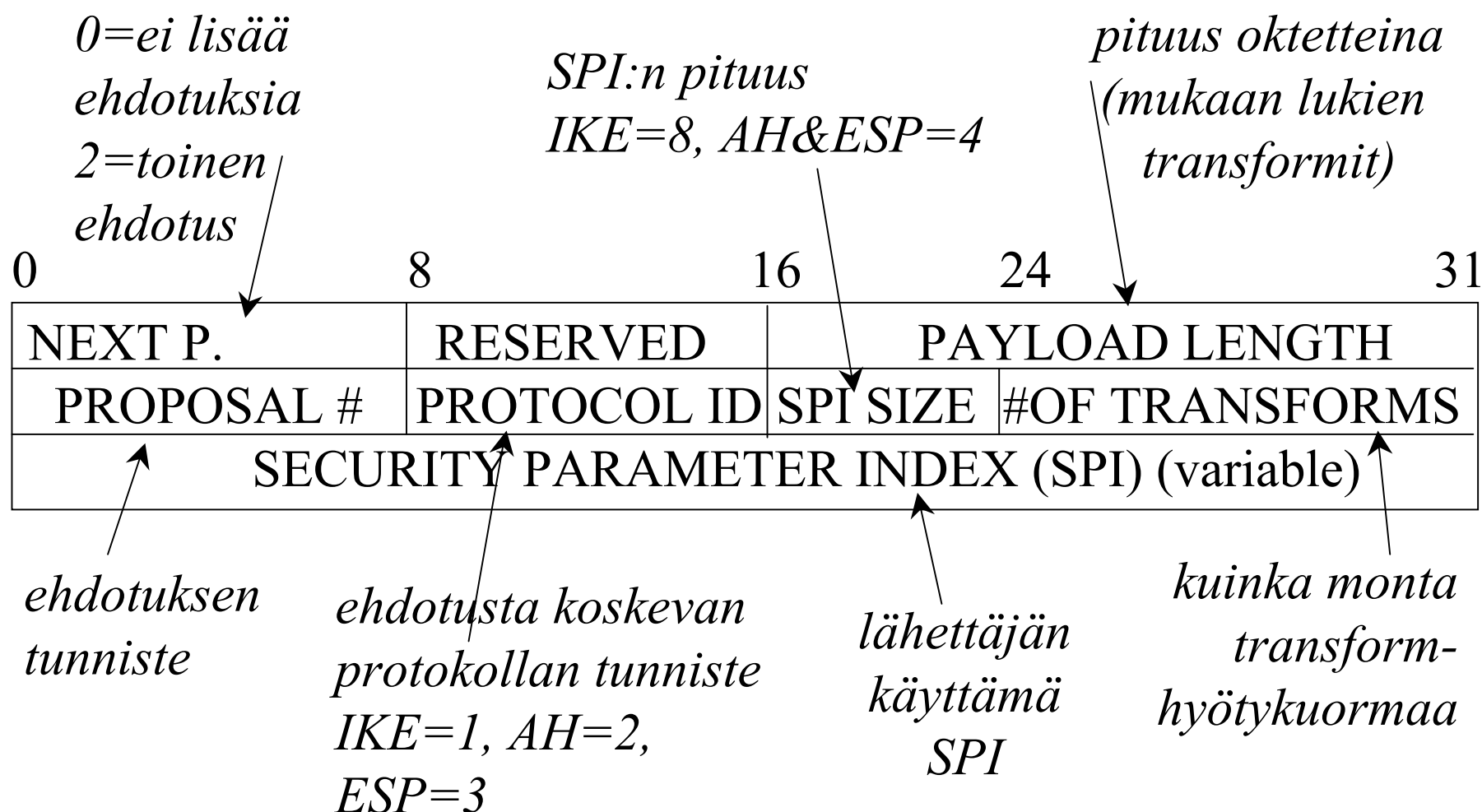
*Oktetteina: tämä otsikko
+proposalit+transformit*



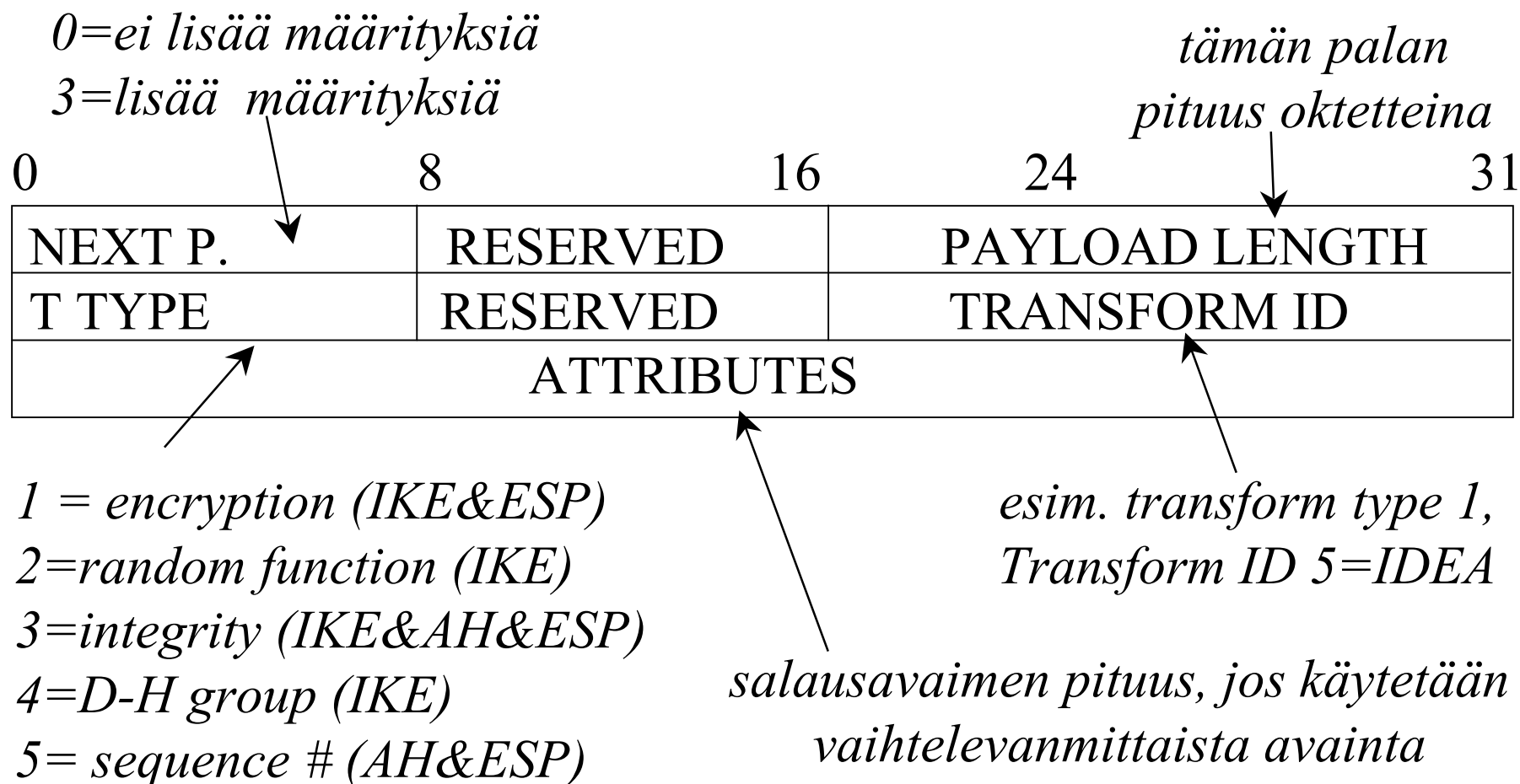
*C=critical
I&ei ymmärretä tätä payloadia
-> hylätään koko viesti*

*Lisäksi yksi tai useampi
Proposal-hyötykuorma*

Proposal Payload (P)

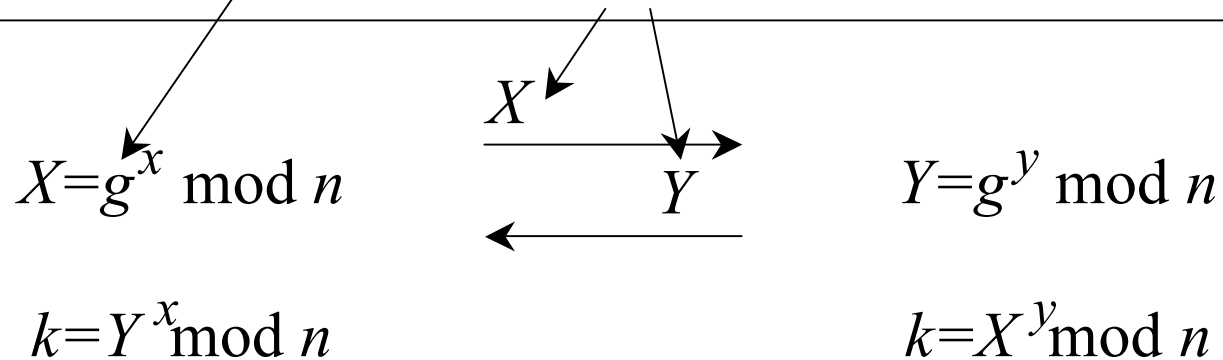


Transform Payload (T)



Key Exchange Payload (KE)

NEXT P.	C	RESERVED	PAYLOAD LENGTH
DH Group #			RESERVED
KEY EXCHANGE DATA			

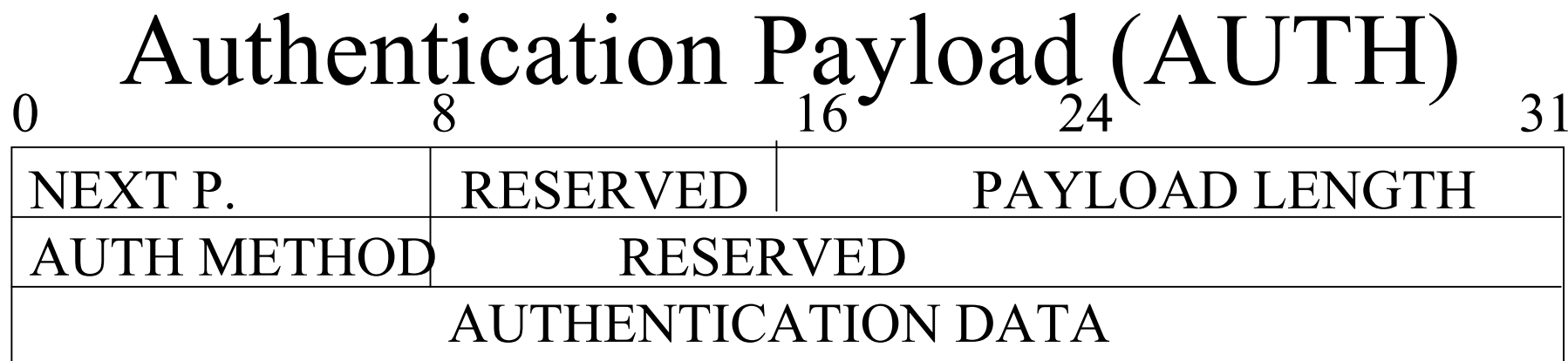


- X, Y, g ja n ovat julkisia, lasketaan nonssien avulla
- x ja y salaisia, ei siirretä verkon yli

Identity Payload (ID)

0	8	16	24	31
NEXT P.	RESERVED	PAYLOAD LENGTH		
ID TYPE	RESERVED			
IDENTIFICATION DATA				

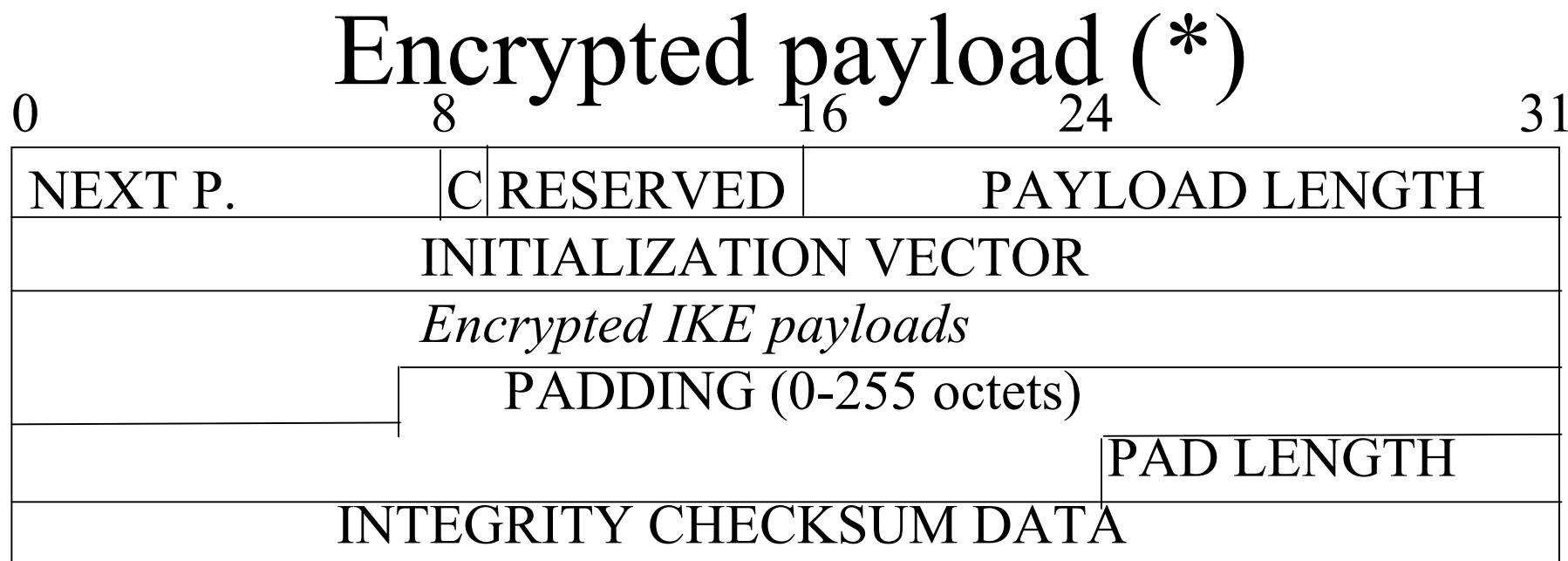
- Käytetään identiteettitiedon vaihtamiseen
 - Osapuolten tunnistaminen
 - Tiedon autenttisuuden määrittämistapa
- ID-tyyppi: 1= IP-osoite, 2=domain-nimi, 3=sähköpostiosoite, 4= IPv6-osoite



- Todennus on allekirjoitus edellisestä viestistä
 - 1 = digitaalinen allekirjoitus RSA:lla
 - 2 = Jaettu avain
 - 3 = digitaalinen allekirjoitus DSS:llä
- Viestissä oleva vastapuolen nonssi takaa tuoreuden



- Sekä sertifikaattien että niiden hallintaan:
 - 1=X.509, 2=PGP, 4=X.509 signature, 9=SPKI certificate, 11=RSA avain
 - 7=Certificate Revocation List (CRL)
 - jne



- NEXT=paketin sisällä olevan tunniste
- Käytetyt algoritmit ja avaimet selviävät otsikon SPI:n avulla

Traffic Selector Payload (TS)

0	8	16	24	31
NEXT P.	RESERVED	PAYLOAD LENGTH		
# of TSs	RESERVED			
<TRAFFIC SELECTOR>				

- Traffic selector:

0	8	16	24	31
TS TYPE	UDP/TCP/ICMP	SELECTOR LENGTH		
START PORT		END PORT		
STARTING ADDRESS				
ENDING ADDRESS				

Traffic Selector (TS)

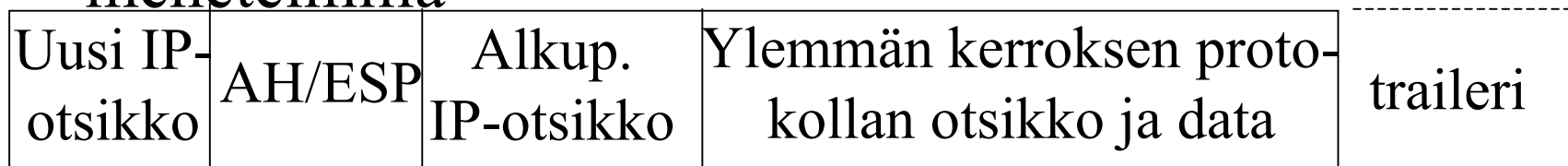
- Hyötykuormaa käytetään vuon tunnistukseen
- TS-tyyppi: IPv4 vai IPv6
- ID Protocol OD: UDP/TCP/ICMP/mikä vaan
- Portit: pienin sallittu porttinumero (tai 0=kaikki sallittu) ja suurin porttinumero (65535 jos kaikki sallittu)
- Osoitteet: osoitealue sallituille osoitteille

IPsec

- Huomaa, että IPsec pitää oikeastaan sisällä myös edellä esitetyn, ei vain seuraavaksi esitetyt asiat
- Kaksi tapaa: tunnelointi ja transport

IPsec-tunnelointi

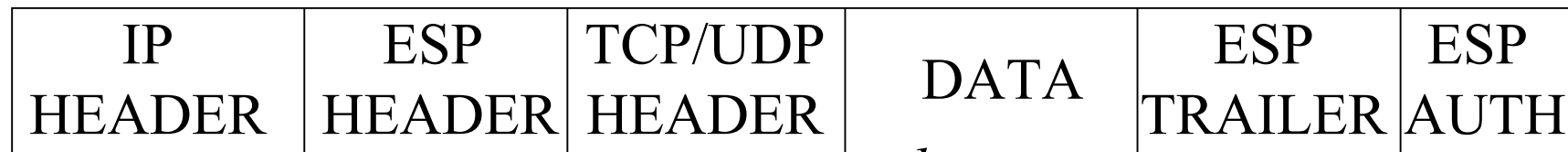
- Tunnelointia käytetään kun toinen tai molemmat yhteyden päätepisteet ovat turva-gatewaytä
- Uusi IP-otsikko lisätään kokonaan suojatun alkuperäisen IP-otsikon (ja IPsec-otsikoiden) eteen
- Koko alkuperäinen paketti on suojattu sovituilla menetelmillä *suojattu* →



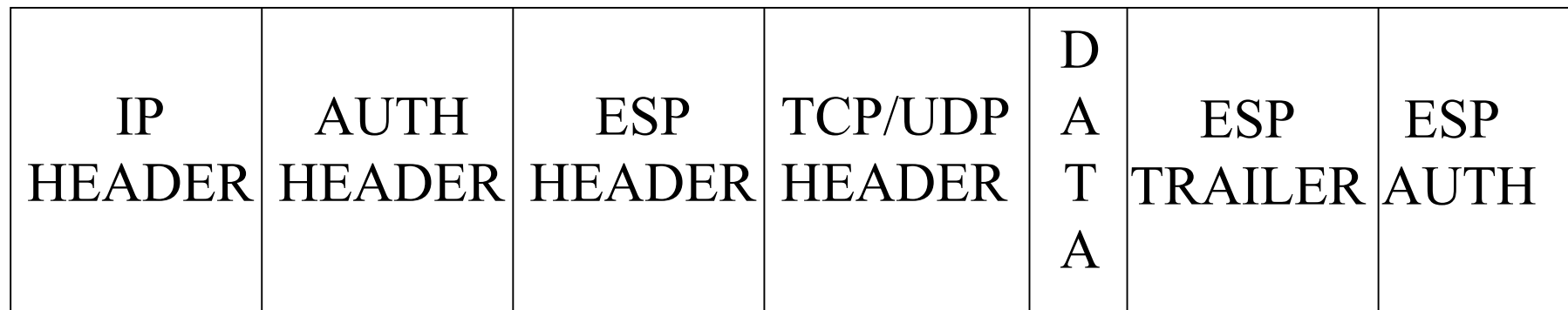
Suojaus (transport mode)



Suojattu muuttamiselta (muuttumattomat kentät)



←—————→ *eheys*
←—————→ *luottamuksellisuus* →



IPsec Authentication Header (AH)

0	8	16	31
NEXT HEADER	PAYLOAD LEN	RESERVED	
SECURITY PARAMETER INDEX (SPI)			
SEQUENCE NUMBER			
AUTHENTICATION DATA ...			

- Yhteydetön eheys ja tiedonlähteen todennus
- Todentaa IP-otsikon muuttumattomat kentät ja tietosähkeen sisällön

IPsec Encapsulating Security Payload (ESP)

0

16

24

31

SECURITY PARAMETER INDEX		
SEQUENCE NUMBER		
PAYLOAD DATA ...		
... PADDING	PAD LENGTH	NEXT HEADER
ESP AUTHENTICATION DATA ...		

- Yhteydetön eheys, tiedonlähteen tunnistus, ja/tai luottamuksellisuus
- Sisältää sekä otsikon että ”trailerin”

SPI ja SA

- Security Parameter Index (SPI kertoo yhteydellä käytetyn SA:n
- Viestin vastaanottajan käyttämä SPI:n
 - vastaanottaja käyttää sitä tietokantahakunsa avaimena
- SA määrittelee käytettävät algoritmit ja avaimet
- SA voi olla erilainen yhteyden eri suuntiin

IPsec-yhteenvedo

- SA:n sopiminen IKE:n avulla
 - SPD:stä politiikkamääritykset
 - Käytetyt SA:t talletetaan SADiin
- Sovitun suojauksen käyttö yhteydellä
 - SPI:n avulla etsitään käytetty SA SAD-tietokannasta
 - IPsec AH ja/tai ESP

Luottamuksenhallinta

- Julkisen avaimen infrastruktuuri (public key infrastructure PKI) tarjoaa todennettuja avaimia
- Sertifikaatit ovat allekirjoitettuja dokumentteja
 - ”tämä julkinen avain kuuluu Teemu Teekkarille”
 - X.509 (identity certificates)
 - SPKI (authorization certificates)
- Luotetut kolmannet osapuolet (trusted third parties TTP)
- Kerberos etc.

Lähteitä

- A. J. Menezes, P. C. van Oorschot, S. A. Vanstone: Handbook of Applied Cryptography
– <http://www.cacr.math.uwaterloo.ca/hac/>
- Pekka Nikander: An Architecture for Authorization and Delegation in Distributed Object-Oriented Agent Systems, väitöskirja 1999

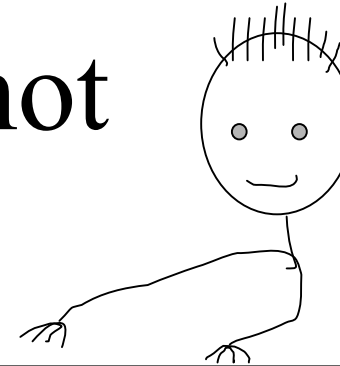
IPsec RFCs

- 4301- Security Architecture for the Internet Protocol, 2005
- 4302 - IP Authentication Header, 2005
- 4303 - IP Encapsulating Security Payload (ESP), 2005
- 4306 - The Internet Key Exchange (IKE), 2005
- 2411 - IP Security Document Roadmap, 1998

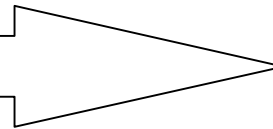
Yhteenveto

- Internet ei ole luotettava (turvallisuusmielessä)
- Useita tekniikoita turvallisuuden toteuttamiselle
- IPsec: todennus ja luottamuksellisuus
- Palomuurit: pääsynvalvonta ja sisäverkon piilottaminen
- Yksityisverkot (VPN): suojattu yhteys Internetin kautta sisäverkkoon (tai sisäverkkojen välillä)

Seuraavat luennot



29.9. TLS &SSH



Sovelluskerros

Kuljetuskerros

Verkkokerros

Linkkikerros

Fyysinen kerros